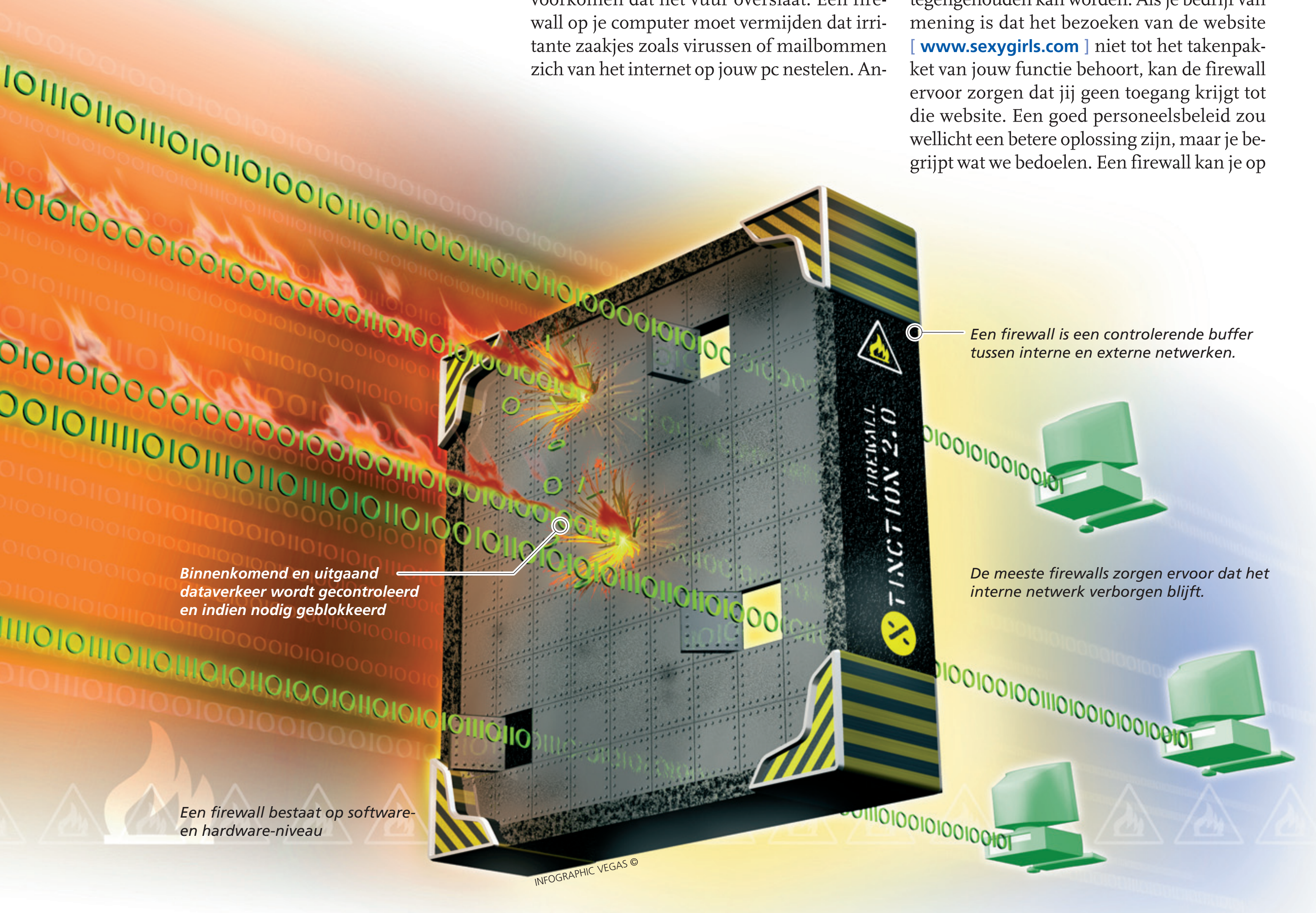
## Wat is het nut van een firewall?

# Vuurvaste bescherm

**Heb je thuis een internetverbinding? Dat betekent dat je computer onrechtstreeks in verbinding staat met miljoenen anderen. Spijtig genoeg heeft niet iedereen even goede bedoelingen. Om je pc tegen allerlei onheil te beschermen, installeer je maar beter een firewall. Zo'n firewall is dan ook het onderwerp van deze 'Hoe werkt'.**

Het woord firewall verwijst naar de vuurvaste begrenzing die aangebracht wordt tussen twee structuren om te voorkomen dat het vuur overslaat. Een firewall op je computer moet vermijden dat irritante zaakjes zoals virussen of mailbommen zich van het internet op jouw pc nestelen. Anders gezegd, een firewall verhindert ongeautoriseerde toegang van óf naar een privé-netwerk. Dat wil zeggen dat ook uitgaand verkeer tegengehouden kan worden. Als je bedrijf van mening is dat het bezoeken van de website [ www.sexygirls.com ] niet tot het takenpakket van jouw functie behoort, kan de firewall ervoor zorgen dat jij geen toegang krijgt tot die website. Een goed personeelsbeleid zou wellicht een betere oplossing zijn, maar je begrijpt wat we bedoelen. Een firewall kan je op



ing

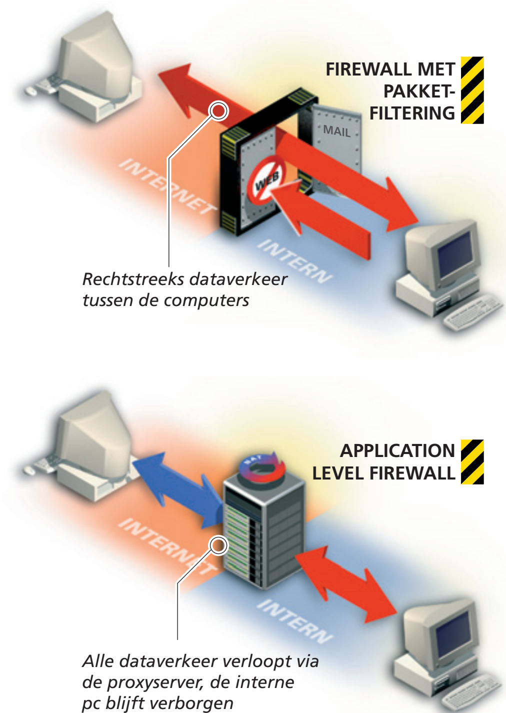
twee manieren instellen: ofwel wordt geen enkel verkeer doorgelaten behalve het verkeer dat jij als veilig gemarkeerd hebt, ofwel wordt alles doorgelaten behalve het verkeer dat jij als onveilig beschouwt. Het spreekt voor zich dat de eerste methode de veiligste is. Voor bedrijven is een firewall een erg efficiënte manier om het interne netwerk te beveiligen. In de praktijk is het immers doorgaans zo dat al het internetverkeer via een centrale gateway of router verloopt. Een router is een gewone pc, met als kenmerk dat die computer het enige verbindingspunt tussen het (veilige) privé- of bedrijfsnetwerk en de (onveilige) buitenwereld of het internet is. Als het bedrijf er vervolgens in slaagt die router goed te beveiligen, is dat heel wat eenvoudiger dan alle computers afzonderlijk te moeten beschermen. Wat een firewall niet doet, is het beschermen van computers tegen de werknemers zelf. Wat bedoelen we daar mee? Wel, de firewall mag dan nog perfect functioneren, als een gefrustreerde werknemer al je bedrijfsgeheimen via een telefoontje naar de concurrentie doorsluist, is je firewall een maat voor niets. Een mooie metafoor: het is zinloos om je tuinhuisje te voorzien van een metalen deur. Je zou kunnen stellen dat confidentiële informatie nooit bewaard mag worden op een computer die op een of andere manier met het internet verbonden is. Dit is vandaag de dag echter niet altijd even eenvoudig te verwezenlijken. Er zijn natuurlijk ook gradaties van vertrouwelijkheid. Overheidsgeheimen moeten nog altijd beter bewaard worden dan je persoonlijke mailbox.

## Misbruik

Wat is nu precies het nut van een firewall voor jou, de thuisgebruiker? Wel, het is toch niet leuk om te merken dat een onbekende lustig doorheen de documenten op je harde schijf bladert? Je hebt toch wel gegevens staan die je liever voor jezelf houdt? Heb je deelgenomen aan één van de voorbije edities van Big Brother en geef je eigenlijk geen barst om je privacy? Bedenk dan dat er nog andere vormen van misbruik bestaan. Zo is er het zogenaamde IP-spoofing, waarbij een hacker jouw computer gebruikt om elders een inbraak te plegen. Wanneer men vervolgens de inbreker probeert te achterhalen, komt men doodleuk bij jou terecht. Nog een reden om een firewall te installeren? Er zijn programma's die al je acties kunnen registreren (loggen). Elke toets die je intikt wordt in een tekstbestandje bewaard. Stel dat je on line een boek gekocht hebt. Dan bevindt jouw VISA-nummer zich in dat bestandje. Voor de hacker is het een koud kunstje om aan de hand van dat tekstbestandje het nummer van je kaart te achterhalen en vervolgens je bankrekening te plunderen. Dit is weliswaar een worst-case-scenario, maar een firewall is dus heus niet alleen iets voor computerfreaks...

## Je eigen nummer

Vooraleer we verder gaan is het noodzakelijk dat je wat inzicht verwerft in de werking van een netwerk. Meer bepaald: hoe weten twee afzonderlijke computers elkaar te vinden, temidden van duizenden andere pc's? In een straat onderscheiden we huizen van elkaar dankzij de huisnummers. Op het internet identificeren we een computer aan de hand van zijn IP-nummer. IP staat voor Internet Protocol, en wijst elke computer softwarematig een uniek adres toe. Een gegevensstroom die via het internet verstuurd wordt, bevat het IP-adres van zowel de ontvanger als de verzender. Op die manier kunnen computers met elkaar communiceren. Een IP-adres bestaat uit vier keer acht bits. Elke bit stelt een nul of een één voor, dus kan je met acht bits 256 verschillende waarden voorstellen. Alle IP-adressen liggen dus tussen 0.0.0.0 en 255.255.255.255. Een IP-adres bestaat uit twee delen: een prefix en een suffix. Het prefix van het adres geeft aan met welk fysiek netwerk de computer is verbonden, terwijl de suffix de individuele computer binnenin dat netwerk aanwijst. Dat is belangrijk, omdat op die manier verschillende computers dezelfde suffix kunnen hebben en toch een uniek adres behouden. Even verduidelijken: stel dat onze computer het IP-adres 192.153.0.1 heeft (het IP-adres van je computer kan je trouwens opvragen door in een DOS-venster het commando IPCONFIG in te tikken). De eerste twee paren van acht bits (192 en 153) stellen bv. het fysieke netwerk van de Belgische overheid voor. Met de twee laatste paren (0 en 1) verwijzen we naar één bepaalde computer binnenin dat netwerk. Waarom is er nu die onderverdeling? Wel, iedere computer moet op elk moment uniek geadresseerd zijn. Om dat te bereiken is er een overkoepelende organisatie die zorgt dat elke netwerkprefix uniek is. Dat is de Internet Assigned Number Authority [ www.iana.org ]. Binnenin een bedrijf kan de netwerkbeheerder alle computers zelf een IP-adres kan toewijzen. Belangrijk is dat dit softwarematig gebeurt: je IP-adres heeft dus niks te maken met het soort computer dat je gebruikt. Nu begrijp je wellicht waarom je computer van een firewall voorzien moet zijn. Wie permanent met het internet verbonden is, beschikt over een vast IP-adres. Dat kan voor hackers een vuurtoren in de duisternis zijn. Er zijn namelijk programma's die het net afstruinen enkel en alleen op zoek naar IP-adressen die niet door een firewall beschermd worden. Ook wie regelmatig inbelt, heeft baat bij een firewall, maar in dat geval verandert het IP-adres wel elke keer dat je inlogt. Dat maakt het voor potentiële inbrekers al wat moeilijker om je te traceren.



*Rechtstreeks dataverkeer tussen de computers*

*Alle dataverkeer verloopt via de proxyserver, de interne pc blijft verborgen*

## Allemaal filters

Allemaal goed en wel, maar hoe werkt een firewall nu precies? We moeten verschillende soorten firewalls onderscheiden. Ten eerste is er de firewall die werkt met **pakketfiltering**. Dat is een programma dat op de router draait en door de netwerkbeheerder geconfigureerd wordt. De netwerkbeheerder stelt een aantal voorwaarden in en enkel indien het pakketje voldoet aan die voorwaarden wordt het doorgelaten. Enkel indien de filter het pakketje expliciet toelaat én ook expliciet niet weigert,

wordt het doorgelaten. Zo kan bv. vastgelegd worden dat enkel e-mailverkeer toegelaten is of dat je enkel mag surfen. Een pakketfilter is de meest eenvoudige, maar ook de snelste soort firewall. Nadeel aan deze firewall is dat de inhoud van de datastroom niet gecontroleerd wordt. Rechtstreeks verkeer tussen twee pc's is dus mogelijk. Een e-mail met een virus wordt dus doorgelaten als mailen toegestaan is.
Een **application level** firewall maakt gebruik van Network Address Translation [ **www.webopedia.com/TERM/N/NAT.html** ]. Die techniek zorgt ervoor dat het voor de buitenwereld niet te achterhalen is van welke computer het verkeer afkomstig is. Dat heeft als voordeel dat informatie over het interne netwerk verborgen blijft. Jouw IP-adres is niet gekend door de ontvanger van je mail. Die krijgt het IP-adres van je router te zien.. Een application-level-firewall zal meestal gebruik maken van proxy's. Een proxy is een programma op de router dat het verkeer voor één bepaalde service (bv. mailen, ftp, http,...) controleert. Proxy's bevinden zich op de proxyserver. Ook hier is dus geen rechtstreeks verkeer tussen de interne en externe pc mogelijk. Al het verkeer verloopt via de proxysoftware op de firewall. Hoe verloopt dat in de praktijk? Wel, jouw pc doet een communicatie-aanvraag bij je proxyserver. Die geeft de vraag door aan de proxyclient van het externe netwerk. Indien die proxyclient de vraag aanvaardt, wordt hij doorgegeven aan de pc op het externe netwerk. Dat is de pc die jij wil bereiken.
Indien het proces in de omgekeerde richting verloopt, wisselen de client en server uiteraard van rol. Wanneer voor een bepaalde dienst geen proxy te vinden is, wordt dat verkeer niet toegelaten. Een application level firewall kan ook data tegenhouden op basis van de inhoud. Zo kan de firewall alle Java-code weigeren. Dit is de veiligste firewall, maar ook het meest belastend voor het systeem. Er moet immers heel wat gecontroleerd worden vooraleer het verkeer doorgelaten wordt.

## Dynamische filter

De veiligheid van pakketfiltering kan verbeterd worden door middel van **dynamische pakketfiltering**, ook wel Stateful Packet Filtering genoemd. Deze filtermethode houdt al het uitgaande verkeer bij en laat enkel de corresponderende antwoorden toe. Aangezien elk datapakketje het IP-adres van de ontvanger bevat, kan de filter eenvoudig controleren of het antwoord afkomstig is van de pc die oorsponkelijk geadresseerd werd. Deze vorm van beveiliging vraagt veel rekenwerk van de computer en is dan ook trager dan de (weliswaar minder veilige) statische pakketfilter. Dit is een dynamische filter omdat de IP-adressen pas tijdens het proces gekend zijn. Dit in tegenstelling tot een statische filter, waar de firewall in een vooraf vastgelegde tabel van toegelaten IP-adressen gaat kijken.
Dan is er ook nog **Stateful Packet Inspection** (SPI). Die techniek kijkt of de inhoud van het als antwoord ontvangen pakketje wel overeenkomt met de inhoud die verwacht wordt. Stel dat je een videoconferentie houdt, dan verwacht de firewall eveneens videobeelden als antwoord. Komt er dan (van hetzelfde IP-adres) een mailtje binnen, dan ruikt dat verdacht veel naar IP-spoofing. SPI is zeer krachtig, maar duur en vergt veel van je systeem. Tot slot onderscheiden we ook nog de **Embedded firewall**. Dat is een netwerkkaartje met geïntegreerde firewall.



*Voor optimale beveiliging kan je een hardware-router installeren.*

Een andere mogelijkheid is een firewall installeren op hardwareniveau. Zo'n router zorgt er ook voor dat al het verkeer sterk gecrypteerd wordt (zie ook Clickx 34). Beveiliging op hoog niveau dus. Daar moet wel stevig voor betaald worden. Zo moet je voor de 3Com SuperStack 3 FireWall [ **www.3com.be** ] € 3.700 neertellen. Daarvoor heb je wel een optimale bescherming en moet je geen pc meer aankopen die als firewall moet dienen. Deze firewall ondersteunt trouwens SPI.

## Hou het veilig

Een veel voorkomende misvatting is dat een firewall een virusscanner overbodig maakt. Wanneer je computer al het verdachte verkeer tegenhoudt, is het toch niet nodig om de bestanden die er wél doorkomen – en dus per definitie veilig zijn – nog eens te gaan scannen? Eerst en vooral is geen enkele firewall waterdicht. Hackers zijn ook wel op de hoogte van de laatste soft- en hardwareontwikkelingen en vinden altijd wel een achterpoortje. Ten tweede is het internet heus niet de enige verspreider van virussen. Wie leent nooit eens een diskette of cd van een vriend of collega? Natuurlijk vertrouwen wij onze beste vrienden, maar het kan best zijn dat hij je per ongeluk met een virus opzadelt. De boodschap mag duidelijk zijn: die scanner heb je nog steeds nodig!
Wie zich nu realiseert dat hij helemaal geen firewall heeft en zijn systeem al aangevallen ziet worden door tientallen hackers, kunnen we wel geruststellen. Windows XP bevat standaard een firewall die je al heel wat bescherming biedt. Die firewall staat standaard echter wel uitgeschakeld. Je kan die natuurlijk zelf activeren. Dat doe je via START, CONFIGURATIESCHERM en het pictogram NETWERKVERBINDINGEN. Rechtsklik op je internetverbinding en kies voor EIGENSCHAPPEN. Om de firewall te activeren moet je onder het tabblad GEAVANCEERD een vinkje zetten voor MIJN COMPUTER EN NETWERK BEVEILIGEN DOOR TOEGANG VANAF HET INTERNET TE BEPERKEN OF TE BLOKKEREN. Rechtsonderaan kan je via de knop INSTELLINGEN de firewall helemaal naar je hand stellen.




*Activeer de firewall in Windows XP.*

Heb je geen XP? Geen nood, op de site van ZoneAlarm [ **www.zonelabs.com** ] kan je een goede én gratis firewall downloaden. Heb je na het lezen van dit artikel zin in méér, surf dan naar [ **www.sans.org/rr/firewall** ] waar je heel wat wetenschappelijke artikels over firewalls terugvindt. Ook Microsoft heeft op zijn website een aparte rubriek voor beveiliging voorzien. Op [ **www.microsoft.com/security** ] vind je de laatste nieuwtjes over virussen, beveiligingslekken en dergelijke. Een veilig systeem hebben is dan wel één zaak, het veilig houden is nog heel wat anders. Heb je een firewall gekocht of geïnstalleerd en wil je weten of die wel werkt? In plaats van je IP-adres op het net te publiceren lijkt het ons beter ShieldsUp en LeakTest even uit te voeren. Beide kan je vinden op [ **www.grc.com** ].
Tot slot: vertrouw altijd op je gezond verstand. Ga alsjeblieft niet in op een mailtje getiteld 'Klik hier om € 5.000 te winnen'. Iemand die je via MSN een programma doorstuurt en je dat per se wil laten uitvoeren, is wellicht ook niet zo te betrouwen. Of een berichtje van je internetprovider die vertelt dat de server is gecrasht. Of je snel even al je gegevens wil doorsturen? Wissen die rommel! En installeer een firewall...

— Benjamin Carlier —